What is claimed is:

Sub a2

CLAIMS

1. A method for verifying, by a verifier, that a prover has access to a private key associated with a public key Kp, the method comprising:

the prover sending an identification message to the verifier, the identification message comprising an indication of an identity of the prover, the indication of the identity including an indication of Kp;

performing an identification round, the identification round comprising:

the verifier choosing a challenge Q and a padding string X;

the verifier sending an initialization message to the prover, the initialization message comprising a disguised form Y produced by applying a public disguising function Fp to Q and X, Y being equal to Fp(Q,X);

the prover computing a random number R by applying a private disguising function Fv to Y, R being equal to Fv(Y);

the prover sending a commit message to the verifier, the commit message comprising a disguised form of R produced by applying a function f to R, the disguised form of R being equal to f(R);

the verifier sending a challenge message to the prover, the challenge message comprising the challenge Q and the padding string X;

the prover verifying that Y=Fp(Q,X);

the prover sending a response message to the verifier, the response message comprising a response A, the response A satisfying a predicate relationship Pred(A,Q,f(R),Kp), wherein satisfying the predicate relationship provides an indication that the prover has access to the private key; and

the verifier verifying that A satisfies the predicate relationship Pred(A,Q,f(R),Kp); and

the verifier determining that the prover has access to the private key based on a result of the performing step.

2. A method according to claim 1 and also comprising:

subsequent to the prover verifying that Y=Fp(Q,X), using the value Fp(Q,X) instead of the value Y of the verifier sending step in all subsequent operations using Y.

3. A method according to claim 1 and wherein the performing step is performed iteratively a plurality of times, and

the verifier determining step includes determining based on a plurality of results each associated with one of the plurality of times that the performing step is performed.

4. A method according to claim 1 and wherein the disguising function Fp comprises a one-way hash function.

5. A method according to claim 3 and wherein the disguising function Fp comprises a one-way hash function.

6. A method according to claim 1 and wherein the private disguising function Fv comprises a one-way hash function.

7. A method according to claim 3 and wherein the private disguising function Fv comprises a one-way hash function.

8. A method according to claim 1 and wherein the public disguising function Fp comprises a public key dependent disguising function Fpp dependent, in part, on the public key Kp, and

Y is equal to Fpp(Q,X,Kp), and

the prover verifying step comprises the prover verifying that Y=Fpp(Q,X,Kp).

9. A method according to claim 3 and wherein the public disguising function Fp comprises a public key dependent disguising function Fpp dependent, in part, on the public key Kp, and

Y is equal to Fpp(Q,X,Kp), and

the prover verifying step comprises the prover verifying that Y=Fpp(Q,X,Kp).

10. A method according to claim 1 and wherein the function f comprises R^2 modulo N.

11. A method according to claim 3 and wherein the function f comprises R^2 modulo N.

12. In a method for verifying, by a verifier, that a prover has access to a private key associated with a public key Kp, in which the method comprises the prover generating a random number R and communicating a disguised form of the random number R to the verifier, an improvement comprising:

the prover generating the random number R based on an input received from the verifier.

13. A method according to claim 12 and wherein the input received from the verifier includes a commitment to a future query, and

the method also comprises:

the prover verifying, upon receipt of the future query, that the future query matches the commitment.

14. A system for verifying access to a private key associated with a public key Kp, the system comprising:

a verifier; and

a prover comprising a disguising unit,

wherein the prover is operative to send an identification message to the verifier, the identification message comprising an indication of an identity of the prover, the indication of the identity including an indication of Kp, and

the prover and the verifier together are operative to perform an identification round, the identification round comprising:

the verifier choosing a challenge Q and a padding string X;

the verifier sending an initialization message to the prover, the initialization message comprising a disguised form Y produced by applying a public disguising function Fp to Q and X, Y being equal to Fp(Q,X);

the prover computing a random number R by applying a private disguising function Fv to Y in the disguising unit, R being equal to Fv(Y);

the prover sending a commit message to the verifier, the commit message comprising a disguised form of R produced by applying a function f to R, the disguised form of R being equal to f(R);

the verifier sending a challenge message to the prover, the challenge message comprising the challenge Q and the padding string X;

the prover verifying that Y=Fp(Q,X);

the prover sending a response message to the verifier, the response message comprising a response A, the response A satisfying a predicate relationship Pred(A,Q,f(R),Kp), wherein satisfying the predicate relationship provides an indication that the prover has access to the private key; and

the verifier verifying that A satisfies the predicate relationship Pred(A,Q,f(R),Kp), and

the verifier is operative to determine that the prover has access to the private key based on a result of the identification round.

15. A prover for use with a verifier for verifying access to a private key associated with a public key Kp, the prover comprising:

a disguising unit,

wherein the prover is operative to send an identification message to the verifier, the identification message comprising an indication of an identity of the prover, the indication of the identity including an indication of Kp, and

the prover and the verifier together are operative to perform an identification round, the identification round comprising:

the verifier choosing a challenge Q and a padding string X;

the verifier sending an initialization message to the prover, the initialization message comprising a disguised form Y produced by applying a public disguising function Fp to Q and X, Y being equal to Fp(Q,X);

the prover computing a random number R by applying a private disguising function Fv to Y in the disguising unit, R being equal to Fv(Y);

the prover sending a commit message to the verifier, the commit message comprising a disguised form of R produced by applying a function f to R, the disguised form of R being equal to f(R);

the verifier sending a challenge message to the prover, the challenge message comprising the challenge Q and the padding string X;

the prover verifying that Y=Fp(Q,X);

the prover sending a response message to the verifier, the response message comprising a response A, the response A satisfying a predicate relationship Pred(A,Q,f(R),Kp), wherein satisfying the predicate relationship provides an indication that the prover has access to the private key; and

the verifier verifying that A satisfies the predicate relationship Pred(A,Q,f(R),Kp), and

the verifier is operative to determine that the prover has access to the private key based on a result of the identification round.